Winston County Schools

Technology Acceptable Use Agreement

COMPUTER SOFTWARE SELECTION AND DUPLICATION

It is the intent of the School District to adhere to the provisions of copyright laws in the area of microcomputer software. It is also the intent of the School District to comply with license agreements and /or policy statements contained in software packages used in the School District. It is recognized that computer software piracy is a major problem for the industry and that violations of computer copyright laws contribute to higher costs and greater efforts to prevent copying and/or lessen incentives for the development of good educational software. All of these results are detrimental to the development of effective educational uses of microcomputers. Therefore, in an effort to discourage violation of copyright laws and to prevent such illegal activities, the following guidelines shall control computer software selection and duplication in the School District:

1. The ethical and practical problems caused by software piracy will be taught to educators and students in all schools of the School District.

2. School District employees will be informed that they are expected to adhere to the provisions of the 1976 Copyright Act as amended in 1980 governing the use of computer software. Section 117 states that the owner of a computer program may make one (1) copy of a program to be used as an archival copy unless licensing provisions obtained with the software state otherwise. Backup copies are not to be used on a second computer at the same time an original is in use simultaneously.

3. Software shall not be placed on a network system without a designated network version or a license agreement. When permission is obtained from the copyright holder to use software on a network system, efforts will be made to secure this software from illegal copying.

4. Illegal copies of copyrighted programs may not be made or used on School District equipment.

5. Any legal or insurance protection of the School District will not be extended to employees who intentionally violate copyright laws.

6. The Superintendent of Schools or designee is the only individual who may sign license agreements for software for schools in the School District. A copy of any software agreement or license shall remain on file at the Central Office.

7. It is the responsibility of the principal at each school site to establish practices that will enforce the School District copyright policies.

8. All staff members (including instructional assistants) will be expected to abide by the provisions of this policy.

9. The Board by this presentation hereby notifies all employees of the intent of this policy.

COMPUTER SOFTWARE USE GUIDELINES

The following computer programs are permissible for use in classrooms throughout the School District:

1. Programs in the public domain.

2. Programs covered by a licensing agreement with the software author, authors, vendor or developer, whichever is applicable.

3. Programs donated or loaned to the school (not illegal copies) and a written record that a bona fide contribution exists.

4. Programs purchased by individual schools and a record that a bona fide purchase exists.

5. Programs purchased by the user and a record that a bona fide purchase exists and can be produced by the user upon demand.

6. Programs being reviewed or demonstrated by the user in order to reach a decision about possible future purchase or requested contribution or licensing.

7. Programs written or developed by School District employees and students for the specific purpose of being used in the classrooms of the School District.

It is also the policy of the School District that there be no copying of copyrighted or proprietary programs on computers belonging to the School District.

SOURCE: Winston County Board of Education, Double Springs, AL
ADOPTED: July 7, 1998
LEGAL REF.: 17 U.S.C. 106; Adapted with permission from policy statement approved by Board of Directors of the International Council for Computers in Education.

STUDENT ACCEPTABLE USE POLICY FOR TECHNOLOGY

The Winston County Board of Education strives to provide an educational environment rich in resources that will enable all students to reach his/her full potential. The Board is offering to those students who agree to act in a considerate and responsible manner, monitored Internet services. You should understand that even the very best Internet filtering software might not block all unacceptable sites, but most educators believe that the benefits to students from access to the Internet far exceed the disadvantages. Access is a privilege, not a right, and requires parental permission.

Misuse and vandalism of equipment, misuse of programs, and/or services will result in restricted or prohibited Internet use and will be punished as defined in the school conduct policies. Further, the system may not be used for commercial purposes to offer, provide, or purchase products or services through the system or use the system for political lobbying or any type of personal financial gain.

The Winston County Board of Education endorses the following student Internet guidelines:

1. PERSONAL SAFETY

a. You will not post contact information or credit information (e.g., address, social security number, driver's license number, date of birth), or any other pertinent personal information.

b. Any contact or receipt of any message you feel is inappropriate or makes you feel uncomfortable should be reported to the network administrator or the sponsoring teacher.

c. Use of unapproved e-mail and chat rooms is not permitted.

d. Use of any unapproved instant messaging service such as Yahoo Pager or MSN messenger is not permitted.

2. ILLEGAL ACTIVITIES

a. You will not attempt to gain unauthorized access to any computer system or go beyond your authorized access by entering another person's ID and password for accession of data files or network resources.

b. You will not deliberately attempt to disrupt the computer system or destroy data by spreading computer viruses or by any other means.

c. You will not post contact information (e.g., address, social security number, driver's license number, date of birth), or any other pertinent personal information that violates the privacy of an individual.

d. You will not attempt to access, modify or delete any data files, folders or system configurations beyond your authorized access.

e. You will not use any network, server or password monitoring equipment or software.

f. No computers/handheld devices should be connected to the network without approval from the Technology Department

3. TECHNOLOGY SECURITY

a. You are responsible for the security of your password, and should take all reasonable precautions to prevent others from being able to use your password. ***Under no circumstances*** should you give your password to another person.

b. You will immediately notify a teacher or the system administrator if you have identified a possible security problem. Do not look for security problems; this may be construed as an illegal attempt to gain access.

c. You will avoid the inadvertent spread of computer viruses and spyware caused by downloading files.

d. Personal software may not be installed or used at the school site.

4. INAPPROPRIATE LANGUAGE

a. On any and all uses of the Internet, whether in application to public or private messages, or material posted on the Web pages, you will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. You will not post information that could cause danger or disruption or engage in personal attacks, including prejudicial or discriminatory attacks. You will not harass another person by a persistent action that distresses or annoys another person and you must stop if asked to do so.

5. RESPECTING RESOURCE LIMITS

a. You will use the system only for educational activities.

b. You will not download, save or print files without permission from a sponsoring teacher.

6. PLAGIARISM AND COPYRIGHT INFRINGEMENT

a. You will not plagiarize words that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.

b. You will not download, copy or install unlicensed software.

7. INAPPROPRIATE ACCESS TO MATERIAL

a. You will not use the Internet to access material that is profane or obscene or that advocates illegal acts or violence or discrimination toward other people.

b. If you mistakenly access inappropriate information, you should immediately tell your teacher or other adult who is designated by the school. This will protect you against a claim of intentional violation of this policy.

c. Your parents should instruct you if there is additional material they think would be inappropriate for you to access. The school system fully expects that you will follow your parents' instruction in this matter.

8. FOR YOUR INFORMATION

a. ***Free Speech***. Free speech as set forth in the school disciplinary code, applies also to your communication on the Internet.

b. ***Search and Seizure***. You should expect no privacy of the contents of your personal files on the Winston County School's system, or the local school network or PCs. Routine maintenance and monitoring of the system can lead to discovery that you have violated this policy, the school code, or the law.

c. ***Due Process***. This school system will cooperate fully with local, state, or federal officials in any investigation related to illegal activities conducted through the Winston County Schools system. In the event of a claim that you have violated this policy, the school disciplinary code, or the law in your use of the Internet, you will be given written notice of suspected violations and an opportunity to present an explanation according to school code and/or state and federal law. Additional restrictions may be placed on your use of the Internet.

The school system makes no guarantee that the functions or the services provided by or through the school system will be error-free or without defect. The school system will not be responsible for any damage you may suffer including, but not limited to, loss of data or interruptions of service. The school system is not responsible for the accuracy or quality of the information attained through or stored on the system. The school system will not be responsible for financial obligations arising from unauthorized use of the system.

When you are using the school network or Internet, it may feel like you can more easily break a rule and not get caught. This is not true. Electronic footprints are imprinted on the system whenever an action is performed. Therefore, you are likely to be caught if you break the rules.

SOURCE: Winston County Board of Education, Double Springs, AL
ADOPTED: July 7, 1998; REVISED: March 14, 2006
LEGAL REF.: The Code of Alabama, 16-8-9, 16-21-1 to 3,

STUDENT TECHNOLOGY USE AGREEMENT COMPLIANCE FORM
Winston County Board of Education

Student

I understand and will abide by the system Technology Use Agreement. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken.

Student Name (please print)_____

Student Signature_____**Date**_____

Parent or Guardian

As the parent or guardian of this student, I have read the Technology Use Agreement. I understand that this access is designed for educational purposes. The Winston County School System has taken precautions to eliminate controversial material; however, I also recognize it is impossible for the Winston County Schools system to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the Internet. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to use the school network and the system Internet and certify that the information contained on this form is correct.

Parent/Guardian Name (please print)_____

Parent Signature_____**Date**_____

Sponsoring Teacher

I have read the Technology Use Agreement and agree to promote this agreement with the student. Because the student may use the Internet for individual work or in the context of another class, I cannot be held responsible for the student's use of the Internet. As a sponsoring teacher, I do agree to instruct the student on acceptable use of the Internet and proper Internet etiquette.

Teacher's Name (please print)_____

Teacher's Signature_____**Date**_____

Please indicate with a check mark whether or not your child may use the Internet.
My child may use the Internet _____ My child **may not** use the Internet _____

TECHNOLOGY USE PRIVILEGES WILL NOT BE GRANTED UNLESS THIS FORM IS RETURNED WITHIN FIVE (5) SCHOOL DAYS.
3/14/06

PARENT ACCEPTABLE USE POLICY FOR TECHNOLOGY

The Winston County Board of Education strives to provide an educational environment rich in resources that will enable all students to reach his/her full potential. The Board is offering to parents who agree to act in a considerate and responsible manner, monitored Internet services. You should understand that even the very best Internet filtering software might not block all unacceptable sites, but most educators believe that the benefits to students from access to the Internet far exceed the disadvantages.

Misuse and vandalism of equipment, misuse of programs, and/or services will result in restricted or prohibited Internet use. Individuals will be held liable for any damage resulting from the misuse of equipment and resources. Further, the system may not be used for commercial purposes to offer, provide, or purchase products or services through the system or use the system for political lobbying or any type of personal financial gain.

The Winston County Board of Education endorses the following parent Internet guidelines:

1. PERSONAL SAFETY

a. You will not post contact information or credit information (e.g., address, social security number, driver's license number, date of birth), or any other pertinent personal information.
b. Any contact or receipt of any message you feel is inappropriate or makes you feel uncomfortable should be reported to the network administrator or the sponsoring teacher.
c. Use of unapproved e-mail and chat rooms is not permitted.
d. Use of any unapproved instant messaging service such as Yahoo Pager or MSN messenger is not permitted.

1. ILLEGAL ACTIVITIES

a. You will not attempt to gain unauthorized access to any computer system or go beyond your authorized access by entering another person's ID and password for accession of data files or network resources.
b. You will not deliberately attempt to disrupt the computer system or destroy data by spreading computer viruses or by any other means.
c. You will not post contact information (e.g., address, social security number, driver's license number, date of birth), or any other pertinent personal information that violates the privacy of an individual.
d. You will not attempt to access, modify or delete any data files, folders or system configurations beyond your authorized access.
e. You will not use any network, server or password monitoring equipment or software.

(continued)

1. **TECHNOLOGY SECURITY**
   a. You are responsible for the security of your password, and should take all reasonable precautions to prevent others from being able to use your password. ***Under no circumstances*** should you give your password to another person.

   b. You will immediately notify a teacher or the system administrator if you have identified a possible security problem. Do not look for security problems; this may be construed as an illegal attempt to gain access.

   c. You will avoid the inadvertent spread of computer viruses and spyware caused by downloading files.

   d. Personal software may not be installed or used at the school site.

2. **INAPPROPRIATE LANGUAGE**
   a. On any and all uses of the Internet, whether in application to public or private messages, or material posted on the Web pages, you will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. You will not post information that could cause danger or disruption or engage in personal attacks, including prejudicial or discriminatory attacks. You will not harass another person by a persistent action that distresses or annoys another person and you must stop if asked to do so.

3. **RESPECTING RESOURCE LIMITS**
   a. You will use the system only for educational activities.

   b. You will not download, save or print files without permission from a sponsoring teacher.

4. **PLAGIARISM AND COPYRIGHT INFRINGEMENT**
   a. You will not plagiarize words that you find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
   b. You will not download, copy or install unlicensed software.

5. **INAPPROPRIATE ACCESS TO MATERIAL**
   a. You will not use the Internet to access material that is profane or obscene or that advocates illegal acts or violence or discrimination toward other people.

   b. If you mistakenly access inappropriate information, you should immediately tell the teacher or other adult who is designated by the school. This will protect you against a claim of intentional violation of this policy.

   c. Parents should instruct their children if there is additional material they think would be inappropriate for them to access. The school system fully expects that students will follow their parents' instruction in this matter.

6. FOR YOUR INFORMATION

a. ***Free Speech***. Free speech as set forth in the school disciplinary code, applies also to your communication on the Internet.

b. ***Search and Seizure***. You should expect no privacy of the contents of your personal files on the Winston County School's system, or the local school network or PCs. Routine maintenance and monitoring of the system can lead to discovery that you have violated this policy, the school code, or the law.

c. ***Due Process***. This school system will cooperate fully with local, state, or federal officials in any investigation related to illegal activities conducted through the Winston County Schools system. In the event of a claim that you have violated this policy, the school disciplinary code, or the law in your use of the Internet, you will be given written notice of suspected violations and an opportunity to present an explanation according to school code and/or state and federal law. Additional restrictions may be placed on your use of the Internet.

The school system makes no guarantee that the functions or the services provided by or through the school system will be error-free or without defect. The school system will not be responsible for any damage you may suffer including, but not limited to, loss of data or interruptions of service. The school system is not responsible for the accuracy or quality of the information attained through or stored on the system. The school system will not be responsible for financial obligations arising from unauthorized use of the system.

When you are using the school network or Internet, it may feel like you can more easily break a rule and not get caught. This is not true. Electronic footprints are imprinted on the system whenever an action is performed. Therefore, you are likely to be caught if you break the rules.

SOURCE: Winston County Board of Education, Double Springs, AL
ADOPTED: March 14, 2006
LEGAL REF.: The Code of Alabama, 16-8-9, 16-21-1 to 3.

EMPLOYEE ACCEPTABLE USE OF SCHOOL TECHNOLOGY POLICY

The Winston County School District is pleased to make available to teachers and support staff access to interconnected computer systems within the District and to the Internet. This network provides access to various School and District educational and management software, educational resources, e-mail, and Internet based resources. In order for the Winston County School District to be able to continue to make its computer network and Internet access available, all teachers and support staff must take responsibility for appropriate and lawful use of this access.

1. PERSONAL RESPONSIBILITY

By signing this Policy, you are agreeing not only to follow the rules in this Policy, but are agreeing to report any misuse of technology equipment, services or data.

2. ACCEPTABLE USES

The use of computers, data files, networked resources, email, and the Internet is for educational, career development and job related purposes only.

3.UNACCEPTABLE USES

a. Uses that violate the law or encourage others to violate the law.
b. Viewing, transmitting, uploading or downloading materials of a violent, dangerous or inappropriate sexual content. Such information might be profane or obscene, advocates or condones the commission of unlawful acts, or advocates or condones violence or discrimination towards other people.
c. Using the computer network for advertising or solicitations by employees, students or outside groups.
d. Access to any computer system beyond your authorized access by entering another person's ID for accession of another person's files.
e. Intruding into the networks or computers of others, and downloading or transmitting confidential information, or copyrighted materials.
f. Failure to protect passwords or sharing passwords that jeopardize the security of the computer network or other networks on the Internet.
g. Intentionally uploading or downloading a worm, virus, "Trojan horse"," time bomb" or other harmful form of programming or vandalism.
h. Intentionally downloading files that contain spy-ware.
i. Participating in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.
j. Creating or forwarding e-mail chain letters or engaging in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
k. Using the network for commercial purposes, financial gain, or fraud.

(continued)

l. Posting contact information (e.g., address, social security number, driver's license number, date of birth), or any other pertinent personal information that violates the privacy of the individual.
m. Use of any unapproved instant messaging service such as Yahoo Pager or MSN messenger.
n. Unauthorized downloading or installation of unapproved software, games, system tools or screensavers.
o. Downloading, copying or installing unlicensed software.
p. The use of network monitoring or auditing equipment or software. The use of monitoring and auditing tools is restricted to the Technology Department for security auditing purposes only.
q. Any modification to network equipment without the approval of the Technology Department. (e.g., servers, switches/hubs, wireless routers/access points)

4. INFORMATION TECHNOLOGY (IT) SECURITY

a. You are responsible for the security of computer(s) assigned to you, this includes: virus and spyware protection, backups of data stored on your computer(s) and the physical security of your computer(s).
b. You are responsible for the security of your user account and password and should take all reasonable precautions to prevent others from being able to use your user account and password. ***Under no circumstances*** should you give your password to another person. Passwords should never be written down, transmitted or stored unencrypted in files or email.
c. Passwords should be changed yearly and meet minimum password standards.
d. A screen/keyboard lock or login screen should be active on all computers when they are not in use.
e. All computer applications that access high risk or confidential data, such as STI, should be closed after each use. High Risk Data is defined as information assets for which there are legal requirements for preventing disclosure of financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA, or the Data Protection Act, are in this classification. Payroll, personnel, student, curriculum and financial information are also in this class because of privacy requirements.
f. Students should never be allowed to access high risk or confidential data.
g. You are responsible for the security of any computer printouts that contains high risk or confidential data that you generate.
h. You are responsible for the security of any media that contains high risk or confidential data files that you create.
i. Computers should be properly shutdown and turned off at the end of the school day.
j. You will immediately notify the system administrator and/or school administrator if you have identified a possible security problem. Do not look for security problems; this may be construed as an illegal attempt to gain access.

5.COMPUTER WORKSTATIONS AND EQUIPMENT

a. Computer workstations should be protected from power fluctuations by the installation of surge protection devices.
b. All computer workstations, laptops and peripheral equipment shall be protected from environmental hazards including, temperature, water, fire, and dust.
c. All computer workstations and peripheral equipment should be shut down and powered off at the end of the day.
d. It is the individual user's responsibility to insure the physical security of computer workstations and peripherals assigned to them.
e. All computer repair and maintenance shall be performed by the technology department.

6.PRIVACY

Network and Internet access is provided as a tool for educational, career development and job related activities. The Winston County School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage.

The school system makes no guarantee that the functions or the services provided by or through the school system will be error-free or without defect. The school system will not be responsible for any damage you may suffer including, but not limited to, loss of data or interruptions of service. The school system is not responsible for the accuracy or quality of the information attained through or stored on the system. The school system will not be responsible for financial obligations arising from unauthorized use of the system.

Yes_____ No_____ I have read and agree to follow the Winston County Schools Employee Acceptable Use of School Technology Policy.

Name (printed): _____ School: _____

Signed: _____ Date: _____

SOURCE: Winston County Board of Education, Double Springs, AL
ADOPTED: March 14, 2006
LEGAL REF.: The Code of Alabama, 16-8-9, 16-21-1 to 3.

WEB PAGE ESTABLISHMENT AND MAINTENANCE

The establishment of web pages by students, faculty, or staff which are to be published on networks owned or controlled by the Winston County Board of Education must adhere to the following guidelines.

1. Each web site must contain the name of the school and a responsible person to contact if mistakes need to be corrected. All web sites must conform to the local community standards of content and design, and conform to all rules and policies of the Winston County Board of Education
2. The use of images, recorded sounds, copyrighted materials, and trademarks is subject to legal restriction. No one may use photographs, video clips, sound clips, or materials which may be subject to copyright, trademark, or trade secret restrictions without written permission of all parties, as applicable.
3. The web page is designed to provide information to people worldwide. The information on the web page will not violate any individual's right to privacy. E-mail addresses, phone numbers, or personal data will not be published unless a written permission is obtained from the individual concerned.
4. No one may use, display, or cause to be disseminated the name "Winston County Board of Education or any subdivision thereof, without prior written permission from the Winston County Superintendent of Education or designee. Web pages should not make any statement to infer or imply official endorsement or approval by the Winston County Board of Education unless prior written permission is obtained.

In the event any web page(s) are discovered which violate any policies or guidelines outlines in this document, the pages will be removed immediately and the violators shall be subject to disciplinary action.

SOURCE: Winston County Board of Education, Double Springs, AL
ADOPTED: December 16, 1999

INTERNET SAFETY

INTRODUCTION

It is the policy of the Winston County Board of Education to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification of minors; and (d) comply with the Children's Internet Protection Act.

DEFINITIONS

Key terms are as defined in the Children's Internet Protection Act.

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in Section 1460 of Title 18, United States Code;
2. Child Pornography, as that term is defined in Section 2256 of Title 18, United States Code; or
3. Harmful to minors.

HARMFUL TO MINORS. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in Section 2246 of Title 18, United States Code.

ACCESS TO INAPPROPRIATE MATERIAL

To the extent practicable, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

INAPPROPRIATE NETWORK USAGE

To the extent practicable, steps shall be taken to promote the safety and security of users of the Winston County Board of Education's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

SUPERVISING AND MONITORING

It shall be the responsibility of all members of the Winston County Board of Education's staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the school principal or designated representatives.

SOURCE: Winston County Board of Education, Double Springs, AL
ADOPTED: Nov. 29, 2001
LEGAL REF.: Children's Internet Protection Act [Pub. L. No. 106-554, 47 USC 254 (h), and 18 USC 1460, 2246 and 2256.

Information Technology Security Policy

I. Scope of the Policy
This policy covers all areas of the Winston County School District, all staff, all students and all other users of the District facilities.

II. Purpose
This document states the information technology security policy of the Winston County School District. Information Technology (IT) as used here includes computer systems and associated devices, networks and communication facilities.

This policy states the conditions of use, the rights and responsibilities of users and administrators and the methods used to implement the policy.

The aim of the policy is to insure:
- Uninterrupted IT services
- The integrity and validity of data
- The ability to recover effectively and efficiently from disruption
- The protection of all Winston County Schools IT assets, including data, software and hardware

III. Physical Security
    a. Computer Servers
        i. All servers shall be located in a secure, lockable room or secure server cabinet.
        ii. Access shall be restricted to authorized personnel for server and network administrative purposes only; visitors should be supervised at all times.
        iii. Protection from electrical failures and fluctuations shall be protected against by the installation of an uninterrupted power supply, (UPS) and surge protection device.
        iv. Server equipment shall be adequately protected from environmental hazards including temperature, water, fire and dust.
        v. It is the schools' administrators' responsibility to insure the physical security of computer servers.
    b. Network Equipment
        i. When financially feasible, network equipment such as switches, hubs, routers and media converters shall be secured in a lockable network cabinet or other secure location that is inaccessible by unauthorized personnel.
        ii. Access shall be restricted to authorized personnel.

iii. All physical, (twisted pair, fiber, wire-less or modem), network installations and upgrades must be approved, performed, or supervised by, the Technology Department.
iv. It is the schools' administrators' responsibility to insure the physical security of network equipment.

c. Computer workstations and peripheral equipment
   i. No computers/handheld devices should be connected to the network without approval from the Technology Department.
   ii. Computer workstations should be protected from power fluctuations by the installation of surge protection devices.
   iii. All computer workstations, laptops and peripheral equipment shall be protected from environmental hazards including, temperature, water, fire, and dust.
   iv. All computer workstations and peripheral equipment should be shut down and powered off at the end of the day.
   v. It is the individual user's responsibility to insure the physical security of computer workstations and peripherals assigned to them.
   vi. All computer repair and maintenance shall be performed by the technology department

IV. Information Security

a. Data Classification - It is essential that all Winston County School data be protected. All data should be reviewed and classified at one of the following three levels of classifications:
   i. All computer applications that access high risk or confidential data, such as STI, should be closed after each use. High Risk Data is defined as information assets for which there are legal requirements for preventing disclosure of financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA, or the Data Protection Act, are in this classification. Payroll, personnel, student, curriculum and financial information are also in this class because of privacy requirements.
   ii. Confidential – Data that would not expose the District to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. The owner of the data is responsible for the security of this data.
   iii. Public – Information that may be freely disseminated.

b. Control of Access to High Risk Information
   i. Access to all computers/networks that access High Risk Information must be controlled by individual and unique login names and authentication passwords.

ii. Each individual user is responsible for the security of their user account and password and will be held responsible for any activity that takes place in their accounts. Any discovered violation or attempted violation of system security must be reported immediately to the Technology Department.
iii. As stated in current acceptable use policies, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username, password, and system access from unauthorized use.
iv. User accounts should be disabled or removed when an employee is no longer employed or assigned to a school site. It is the responsibility of the local school administrator to notify the technology department when accounts need to be closed.
v. Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
vi. A screen/keyboard lock or login screen should be active on all machines when they are not in use.
vii. All connections or software that access High Risk Information data must be closed when not in use. Minimizing to the task bar is not acceptable.
viii. All High Risk Information data shares must be protected by share access controls that allow only authorized users' access to the shares.
ix. Only authorized users should attempt access to High Risk Information.
x. Students should never be allowed access to any High Risk Information except for curriculum software where an authorized system administrator has assigned them a unique username and password that allows them access to course work or test assigned to them.
xi. Computer generated printouts that contain High Risk Information must be protected from unauthorized access or copying. Printouts containing High Risk Information must be shredded prior to disposal.
xii. Computer removable media that contains High Risk Information must be stored in a protected area that prevents access. High Risk Information backups should be encrypted when feasible to add an extra level of security. Removable media containing High Risk Information must be destroyed prior to disposal.

c. Passwords
i. All users of systems that contain High Risk Information must have a strong password.
ii. All server administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt or reconfigured.
iii. Passwords must not be placed in emails unless they have been encrypted.

iv. System – server level administrative passwords should be changed on a regular basis as specified by the Technology Department.
v. User level passwords should be changed yearly at minimum or when specified by the Technology Department.
vi. User passwords should meet the following standards:
    1. A minimum of seven alphanumeric characters.
    2. Contain both upper and lower case characters.
    3. Include special characters (e.g. @#$%^&*()_+).
vii. Passwords should not contain:
    1. A word in any language, slang, dialect, jargon, etc.
    2. Personal information, names of family, pets, etc.
viii. When changing passwords the reuse of the previous three passwords is not allowed.
ix. Passwords should never be written down or stored on-line.
x. Do not use the "Remember Password" feature of applications.
xi. The use of password auditing/cracking software is restricted to the Technology Department for security auditing purposes only.

d. Acceptable Use of Computer and Network/Internet Resources
    i. All employees of the Winston County Schools must sign an acceptable use policy.
    ii. All students and their parents must sign an acceptable use policy each school year.

V. Information Loss Prevention
a. Data Backup
    i. Backup of all High Risk Information must be completed on a regular basis and stored in a safe and secure manner that protects the data and meets disaster recovery requirements.
    ii. Backups must include multiple generations of data.
    iii. It is the responsibility of school administrators to ensure data backups are being performed at their school.
b. Virus Protection
    i. The willful introduction of computer viruses or disruptive/destructive programs into the Winston County Schools environment is prohibited, and violators may be subject to prosecution.
    ii. All desktop and laptop systems that connect to the network must be protected with approved, licensed anti-virus software that is kept updated. It is the responsibility of each individual user to insure his/her computer is protected and has up-to-date virus definition files, and will be held accountable for any virus activity that takes place on their computer.

iii. All servers that connect to the network must be protected with approved, licensed anti-virus software and kept updated. It is the responsibility of the server administrator to insure anti-virus software is installed and active with up-to-date definitions files.
iv. All removable media, floppies, CD's, USB drives, etc. from an external source must be virus scanned before they are used within Winston County Schools.
v. Incoming e-mail should be scanned when financially feasible to implement.
vi. When feasible, system or network administrators will inform users when a virus has been detected.

c. Spy-ware protection – It is the responsibility of all users to scan their computer on a regular basis for spy-ware. It is the responsibility of the Technology Department to provide spy-ware scanning and removal tools.
d. Firewall
    i. At minimum, a firewall should be installed that protects the Winston County Schools network from intrusion from the outside world.
    ii. When financially feasible, an additional layer of firewalls should be installed to protect servers housing data classified as High Risk Information from potential internal security threats.
e. Intrusion Detection
    i. When financially feasible, intrusion detection software should be installed on all servers housing data classified as High Risk Information.
    ii. The use of intrusion detection software is restricted to the Technology Department for security auditing purposes only.
f. Auditing
    i. Operating systems and application software event logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems, must be enabled.
    ii. The use of LAN analyzer equipment and software is restricted to the Technology Department for security, maintenance and troubleshooting purposes only.
    iii. Server, firewall, and critical system logs should be reviewed frequently.
g. Internet Security.
    i. All connections to the Internet, (including dial-up and wireless), must go through a properly secured connection point to ensure the network is protected when the data is classified as High Risk or Confidential.
    ii. Internet and other external access is restricted to authorized personnel only. Only staff and students with signed Acceptable Use Policies are authorized to access Internet resources.

h. System Security
    i. All server installations and upgrades must be approved and performed or supervised by the Technology Department.
    ii. All server-networked applications must be approved and installed or supervised by the Technology Department.
    iii. All systems connected to the Internet should have a licensed vendor-supported version of an operation system installed.
    iv. The use of unauthorized software is prohibited. In the event of unauthorized software being discovered, it will be removed from the computer immediately. The Technology Department should be consulted if software is in question prior to installation.
    v. All systems connected to the Internet must be current with security patches.
    vi. Regular system integrity checks of host and server systems housing High Risk Information should be performed.

VI. Disaster Recovery
    a. When financially feasible, a documented and tested disaster recovery plan should be established for each site and server that stores High Risk Information.
    b. At minimum, backups of data and applications should be maintained at an offsite location. Data backups maintained offsite should be updated at a minimum of once a week. Application backups should be updated as new versions are installed.

VII. Sanctions
    a. Computers, labs or network segments on the Winston County Schools network will be disconnected if they are deemed by the Technology Department to be a security threat or danger to the remainder of the LAN / WAN.
    b. Penalties for violation of this policy range from loss of computer resource usage privileges to expulsion for students or dismissal for employees. Each case will be determined separately on its own merits.

SOURCE: Winston County Board of Education, Double Springs, AL
ADOPTED: March 14, 2006